UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP.,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING COMPUTER BOTNETS AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS,

Defendants.

ORDER ADOPTING REPORT AND RECOMMENDATION

20-CV-1217 (LDH) (RER)

LASHANN DEARCY HALL, United States District Judge:

This matter came before the Court on Plaintiff's Microsoft Corporation ("Microsoft") Motion for Default Judgment and Entry of Permanent Injunction. On May 28, 2021, United States Magistrate Judge Ramon E. Reyes, Jr. issued a Report and Recommendation (Dkt. 19), recommending that Plaintiff Microsoft Corp.'s ("Microsoft") motion for default judgment be granted and convert the Court's preliminary injunction into a permanent injunction as outlined in Microsoft's proposed order (Dkt. 18-2). Microsoft served Magistrate Judge Reyes, Jr.'s Report and Recommendation on all parties on June 4, 2021. No objections have been filed by any party.

Having reviewed the report and recommendation, Microsoft's briefing on the motion, and the entire record in this matter, this Court finds that Magistrate Judge Reyes Jr.'s Report and Recommendation is well founded in law and consistent with this Court's own view of the evidence in the record. Acting on the recommendation of Magistrate Judge Reyes, Jr., **IT IS HEREBY ORDERED AND ADJUDGED** that, pursuant to Title 23, United States Code, Section 636(b)(1)(C), the "Report and Recommendation Regarding Microsoft Corp.'s ("Microsoft") Motion for Default Judgment and Permanent Injunction" (Dkt. 19) is adopted in its entirety and as ordered herein.

Microsoft has established the elements of its claims pursuant to: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq*.; and (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a). Defendants John Does 1-2 ("Defendants") failed to appear, plead, or otherwise defend this action. Microsoft is entitled to default judgment under Rule 55(b) and a permanent injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Motion for Default Judgment and Entry of Permanent Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This action involves malicious activity carried out by two unidentified Defendants who use the Necurs Botnet ("Necurs") to harm computing devices running on Microsoft's Windows operating system.

2. A 'botnet' is a collection of individual computing devices infected with malicious software ("malware") that allows communication among those devices and centralized or decentralized communication with server computers that provide control instructions." The botnet at issue here—Necurs—is a global botnet, comprised of computing devices connected to the internet, that distributes spam and malware.

3. Computing devices that run on Microsoft's Windows operating system have been forcibly connected to Necurs, which degrades the integrity of the system, disables its antivirus software, and carries out malicious actions from those computers without the knowledge of the

device owners and users. Necurs malware makes changes to "the deepest and most sensitive levels of the [infected] device's operating system." This includes altering the normal and approved Windows settings such that it destabilizes the operating system. As a result, the Windows operating system no longer operates normally, although it continues to bear the Windows and Microsoft marks. As a result, the Necurs malware transforms the Windows operating system into a counterfeit product. In the eyes of the user of the Windows operating system, Necurs becomes Microsoft, but it is not Microsoft at all. Nor is the user aware that Necurs is manipulating their devices to commit cybercrimes.

4. Necurs has infected over nine million end user computers.

5. Defendants were properly and adequately served with Microsoft's summons, complaint, and other pleadings in this action by email and through publication to the Necurs notice website (noticeofpleadings.com/NECURS). Service by email and publication on the Necurs notice satisfied Due Process, satisfied Fed. R. Civ. P. 4 and was reasonably calculated to provide Defendants with notice. *See AMTO, LLC v. Bedford Asset Mgmt., LLC,* No. 14 Civ. 9913 (KMK), 2015 WL 3457452, at *7 (S.D.N.Y. June 1, 2015).

6. Defendants failed to appear, plead, or otherwise defend against this action.

7. This Court has jurisdiction over the subject matter of this case and venue is proper in this judicial district.

8. Microsoft is entitled to entry of judgment and a permanent injunction against Defendants.

9. The record evidence indicates that no Defendant is an infant or incompetent.

10. Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications

Privacy Act (18 U.S.C. § 2701), and the Lanham Act (15 U.S.C. §§ 1114, 1125).

11. Microsoft owns the registered trademarks "Microsoft" and "Windows" used in connection with its services, software and products. Those subject marks are strong, distinctive, and exclusively identify Microsoft's businesses, products, and services.

12. The evidence set forth in the record demonstrates that Defendants have engaged in violations of the foregoing law by:

a. using Microsoft's registered trademarks in bad faith in order to alter the operating systems of infected computers, including their anti-virus software and Windows registry, but it does not make changes to the appearance of the Microsoft or Windows marks

b. cause the Necurs malware to make copies of Microsoft's trademarks onto infected devices, in the form of file names, domain names, target names, and/or registry paths that contain the "Microsoft" and "Windows" marks

c. intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to

i. install on those computers and computer networks malicious code and thereby gain control over those computers and computer networks in order to make them part of a botnet;

ii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing authentication credentials, monitoring the activities of users, and using other

instrumentalities of theft;

iii. steal and exfiltrate information from those computers and computer networks;

d. deploying computers and Internet domains to establish a command and control infrastructure by which means Defendants conducts illegal activities, including (i) installing malicious code on computers and computer networks in order to make them part of a botnet, (ii) sending unsolicited spam e-mail to Microsoft's email services, (iii) sending unsolicited spam e-mail that falsely indicates that they are from or approved by Microsoft, (iv) delivering malicious software designed to steal financial account credentials, (v) delivering malicious "ransomware" software designed to lock access to computers and demand a ransom from victims, (vi) carrying out fraudulent schemes, (vii) monitoring the activities of users and stealing information from them, and (viii) attacking computers and networks, monitoring activities of users, and theft of information;

e. corrupting Microsoft's operating system and applications on victims' computers and networks, thereby using them to carry out the foregoing activities.

13. Defendants have no lawful interest in continuing the activities set forth in the record. In the absence of a permanent injunction, Necurs would regain access to the infected computer devices and begin to operate again. The continued operation of Necurs would cause Microsoft to lost control over the reputation of its Microsoft and Windows trademarks and cause irreparable harm to Microsoft, Microsoft's customers, and the public.

14. Defendants have engaged in illegal activity using the Internet domains identified in **Appendices A** and **B** to the March 5, 2020 Temporary Restraining Order (Dkt. 6-3, 6-4, 6-5, 6-6, 6-7, 6-8), which are incorporated herein by reference, to host the command and control software and content used to maintain and operate the botnet. To halt the injury caused by Defendants, ownership of Defendants' registered domain set forth in **Appendix A** must be permanently transferred to Microsoft and that registration of the domains set forth in **Appendix B** must be prevented.

15. The hardship to Microsoft and its customers that will result if a permanent injunction does not issue weighs in favor of an injunction. Defendants will suffer no cognizable injury as a result of being enjoined from further illegal conduct.

16. An injunction to prevent further illegal conduct by Defendants is in the public interest.

17. Microsoft has served copies of the Court's Report and Recommendation (Dkt. 19) by alternative means. Specifically, Microsoft has served copies of the Report and Recommendation by email and through publication on the Necurs notice website.

IT IS THEREFORE ORDERED that, Microsoft's Motion for Default Judgment and Entry of a Permanent Injunction is Granted.

IT IS FURTHER ORDERED that Defendants are in default, and that judgment is awarded in favor of Microsoft and against Defendants.

IT IS FURTHER ORDERED that Defendants, their representatives and persons who are in active concert or participation with them are permanently restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft's customers and associated member

organizations, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the Internet domains, domain name servers, and IP addresses; (6) downloading or offering to download additional malicious software onto the computers of Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

IT IS FURTHER ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are permanently restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Microsoft" and "Windows" and/or other trademarks, trade names, service marks, or Internet Domain addresses or names; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

IT IS FURTHER ORDERED that Defendants shall forfeit ownership and control of the domain identified in **Appendix A** to the March 5, 2020 Temporary Restraining Order to Microsoft.

IT IS FURTHER ORDERED that, with respect to the discrete set of dynamically generated domains set forth at **Appendix B** to the March 5, 2020 Temporary Restraining Order, that are being generated and will be generated by the botnet code for a period of 25 months from the date of this order, pursuant to stipulation and pursuant to the All Writs Act (28 U.S.C. § 1651), the domain registries shall take the following actions:

A. The domain registry and service provider Neustar, Inc., Afilias USA, Inc., Public Interest Registry and ICM Registry LLC, identified in **Appendix B** to the March 5, 2020 Temporary Restraining Order, shall take reasonable steps to prevent such domains from entering the zone file, consistent with its operational capabilities in order to prevent the domains from being controlled by the Defendants or third parties. Means of compliance with this term include, but are not limited to, implementation of proprietary systems by Neustar, Inc., Afilias USA, Inc., Public Interest Registry and ICM Registry LLC that automatically prevent registration of domains, or pre-registering such domains in an Afilias USA, Inc. "house account" or other means reasonably calculated to prevent registration of the dynamically generated domains by Defendants or any third party. "Dynamically generated domains" shall mean the discrete list of domains automatically generated by the botnet software running on test machines in a laboratory environment and which is not subject to discretion. Nothing in the foregoing shall prevent registration or activation of the domains by Microsoft or its security industry partners Stichting Registrar of Last Resort Foundation and The Shadowserver Foundation for purposes of analysis of the botnet.

B. The domain registry and service provider Verisign, Inc., identified in **Appendix B** to the March 5, 2020 Temporary Restraining Order, shall take reasonable measures, at the registry's discretion, to cause the dynamically generated domains in **Appendix B** to the March 5,

2020 Temporary Restraining Order to be unresolvable. "Dynamically generated domains" shall mean the discrete list of domains automatically generated by the botnet software running on test machines in a laboratory environment and which is not subject to discretion. Nothing in the foregoing shall prevent registration or activation of the domains by Microsoft or its security industry partners Stichting Registrar of Last Resort Foundation and The Shadowserver Foundation for purposes of analysis of the botnet.

C. The foregoing domain registries shall treat any domain names set forth in **Appendix B** of the March 5, 2020 Temporary Restraining Order that have been registered as if they are included in **Appendix A** to that order, unless otherwise instructed by Microsoft or its delegates.

SO ORDERED

Dated: Brooklyn, New York
September 20, 2021

/s/ LDH
LASHANN DEARCY HALL
United States District Judge